Remote Controlled Garage Door Opening System

Field of The Invention

This invention relates generally to garage door openers, more particularly to remotely controlled systems for opening and closing garage doors, gates and the like, and even more particularly to systems of this type which provide increased security from unauthorized access.

Background of The Invention

The use of remote control systems to operate barriers, such as garage doors, gates and the like, is well known. Such remote control systems typically utilize hand held transmitters which emit encoded signals transmitted at radio frequencies to a receiver associated with an automatic door or gate operator. The receiver is effective to intercept and decode the transmitted signal and thus cause the actuation of the operator to open or close the door or gate. These systems include the type in which the receiver has code switches which can be manually set to correspond to the authorized transmitter codes or, alternatively, may be "learn" type systems in which codes or the like used to identify authorized transmitter codes are initially stored in the receiver during a preparatory program or learn mode.

The risk of unauthorized access is a major concern associated with the use of the above mentioned systems. For example, unauthorized access can potentially be achieved by means of an exhaustive, systematic search in which a large number of different codes are successively transmitted in the hope that, eventually, one of the transmitted codes will match the authorized code and activate the system. Another scheme used to gain unauthorized access is a technique, sometimes referred to as "code grabbing", in which the initial transmission of the authorized code is electronically intercepted and stored for later unauthorized use.

Many of the prior art remote control systems have been susceptible to unauthorized access by one or both of the above described methods. For

example, U.S. Patent No. 4,750,118 issued June 7, 1988 to Heitschel *et al.* discloses one type of "learn" remote control system for operating a garage door opener, but one particularly susceptible to code grabbing, in that each transmitter unit of the disclosed system has its own unique, but non-changing code. Accordingly, since each transmitter unit sends the exact same coded signal to activate the door operator every time it is used, the system of the Heitschel *et al.* patent is vulnerable to having the code intercepted and later used to gain unauthorized access.

The system of the type disclosed in the Heitschel *et al.* patent has additional disadvantages which inhibit its effectiveness. For example, the means used to transfer between the program (learn) mode and the operate mode comprises a two-position mechanical switch disposed on the operator power head housing suspended from the garage ceiling, and which must be manually moved between program and operator positions to place the receiver in either the "learn" or "operate" mode. Moreover, the means used to enable receiver storage of codes from different transmitters is also a multi-position mechanical switch which must be manually moved to the desired position prior to receipt of the particular transmitter code. Such arrangements are awkward and inconvenient and, as will be appreciated by those skilled in the art, potentially unreliable.

Barrier (garage door or gate) control systems which use a technique known as code hopping or code stepping are also known and have been previously described and used as a means for preventing unauthorized access by so-called "code grabbing". In accordance with this code hopping technique, the code that activates the system changes (*i.e.*, steps or hops) after each use. For example, one particular advantageous form of code hopping is described in U.S. Patent No. 5,517,187 to Bruwer *et al.*, assigned to an assignee of the present invention. However, a code hopping technique in accordance with the present invention as well as the manner by which it is incorporated with the design and operation of

the remote system itself, uniquely distinguishes the total system of the present invention from prior art systems.

Accordingly, a need for further improvements in remote controlled door and gate operator systems has continued to be felt.

It is therefore a principal object of the present invention to provide a new and improved remote control door and gate operating system. Another object is to provide such a remote control operating system with improved means for preventing unauthorized access, including code grabbing. A still further object of the invention is to provide such a system which avoids the disadvantages and inconveniences associated with prior art systems utilizing mechanical or manually actuated switches.

Other objects and advantages of the invention will become apparent from the following specification, accompanying drawings and claims.

Summary of The Invention

In accordance with a key feature of the present invention, a form of code hopping embodying a unique sequential decryption/comparison technique is incorporated into the operation of a remote control system for activating barrier opening apparatus, particularly garage door or gate openers. In addition, the remote control system is of a "learn" type, but one in which the authorized operating codes stored in the receiver during the learn mode are never themselves transmitted from the transmitter.

Broadly stated, the remote control system of the present invention comprises one or more RF transmitters and a digital type RF receiver associated with the door operator. The receiver is initially programmed with a "manufacturer's key" value. Every system produced by a given manufacturer has the same manufacturer's key. In addition, each transmitter is initially programmed with a unique serial number and unique "secret key". The secret

key stored in the transmitter is generated using the unique serial number of the transmitter and the manufacturer's key. Thus, every transmitter has a different serial number and a different secret key. When the transmitter is activated, it performs a nonlinear encoding function using the secret key to generate a changeable hopping code signal. The hopping code changes (*i.e.*, hops) every time the transmitter is activated.

The transmitter's unique secret key is never transmitted, and although the transmitter's unique serial number is transmitted, it is not stored in the receiver. In accordance with a feature of the invention, the secret key value which is stored in the receiver is self-generated in response to the encoded transmission from the transmitter during the program or learn mode of the receiver. During the subsequent operate mode, the receiver then uses the previously generated and stored secret key to decode the hopping code signal from the transmitter. The door operator or opener device is activated when such decoded information is within a "window" or range of acceptable values as determined by a sequential comparison technique subsequently described.

In accordance with other unique features of the system of the invention, the transition of the receiver between the operate mode and the learn mode is effected by means which momentarily places a microprocessor associated with the receiver in the learn mode, followed by the automatic return of the microprocessor to the operate mode without any further action required of the user. In addition, the system of the present invention enables a technique of random storage in unused receiver memory to accommodate codes from different transmitters rather than requiring the receiver to be "switched" to a different memory location for a given transmitter.

The present invention also provides a remote control door or gate operating system which is more convenient to operate, in all modes, than prior art systems. Those skilled in the art will further appreciate the invention upon reading the detailed description which follows in conjunction with the drawings.

Brief Description of the Drawings

The invention will now be described, by way of a nonlimiting example, with reference to the accompanying drawings in which:

FIG. 1 is an illustration of a remote controlled garage door operating system of the type in which the present invention is incorporated.

FIG. 2 are block diagrams of a transmitter and receiver of the system of the present invention.

FIG. 3 is an illustration of the data flow related to the initial programming of a transmitter in accordance with the principles of the present invention.

FIG. 4 is an illustration of the data flow related to the initial programming of the receiver in accordance with the principles of the present invention.

FIG. 5 is an illustration of the data flow associated with the encryption function in accordance with the principles of the present invention.

FIG. 6 is an illustration of the data flow associated with the decryption function in accordance with the principles of the present invention.

FIG. 7a is an illustration of the data format of the coded signal transmitted by the transmitters of the system of the present invention.

FIG. 7b is an illustration of the data format of the coded signal utilized by the receiver of the system of the present invention when operating in the program or learn mode.

FIG. 7c is an illustration of the data format of the coded signal utilized by the receiver of the system of the present invention when operating in the operate mode.

Detailed Description of the Preferred Embodiment

FIG. 1 shows an embodiment of a remote controlled garage door system 1 of the present invention used for remotely automatically activating (opening and closing) a garage door. The system described hereinafter can also be used as a remote control system for actuating a gate or virtually any other type of movable barrier. System 1 comprises a plurality of transmitters 40 and power head operator 20 normally suspended from the ceiling of the garage. Rail 22 extends

from power head 20 and is secured to the wall above the garage door 24. A first end of door arm 26 is joined to door 24, and a second end of door arm 26 is adapted to reciprocate along the length of rail 22. Power head 20 contains a drive mechanism 64, as is known in the art, for reciprocatively moving (by chain not shown) along rail 22 for opening and closing garage door 24.

The drive mechanism 64 can be activated in conventional fashion by pressing button 30 of wall unit 31. Alternatively, the drive mechanism 64 can be remotely activated by one of the transmitters 40 which, upon actuation, transmit coded radio frequency signals to a receiver 42 (FIG. 2) in power head operator 20, all conventionally known.

The system of the present invention is a learn type system by which the receiver 42 is effected to alternate between a program or learn mode, during which codes or coded values are created and stored which will be used to identify authorized transmitter codes, and an operate mode during which the said identification process is carried out.

With reference to FIG. 2, each transmitter 40 can be activated by buttons 44, which are operable to cause the transmitter to perform various functions. In the preferred embodiment, each transmitter comprises up to four buttons 44 with various functions described in more detail below. Each transmitter 40 contains transmitter control circuitry 46 (which can be a custom integrated circuit), encoding circuitry 48, memory 50, and RF transmitter circuitry 52 including a suitable antenna 52a for generating and transmitting an encoded transmission signal. The receiver 42 contains RF tuning circuitry 54 connected to a suitable receiving antenna 54a, decoding circuitry 56, memory 58 and activation circuitry 62 to activate drive mechanism 64 in response to the identification of an authorized transmitter code. In addition, as described below in greater detail, a learn mode button 60 can be used by the operator to initiate the learn mode of the receiver. As shown in FIG. 2, a microprocessor 55 of conventional design and construction is used for controlling the operation of receiver 42.

The transmitter 40 is operable to transmit an encrypted hopping code signal that changes with each transmission. The receiver 42 is operable to receive and decrypt the encrypted hopping code signal and to activate drive mechanism 64 when the decrypted signal identifies the presence of an authorized transmitter code. The encoding and decoding functions respectively performed by the encoding circuitry 48 and decoding circuitry 56 employ novel variations of the code hopping technique disclosed in U.S. Patent No. 5,517,187 to Bruwer, *et al.*, which by this reference is incorporated herein for all purposes.

Initial Programming

By way of example, each transmitter 40 is initially programmed with the following: (a) a twenty-four bit "serial number", (b) a sixty-four bit "secret key", (c) a "check" value and (d) an initial synchronization value. Each transmitter has a unique twenty-four bit serial number and a unique sixty-four bit "secret key". The check value is simply a fixed value, and it remains the same for each transmission of the transmitter 40. The synchronization value is a sixteen bit binary number which increments, in this preferred embodiment by one, every time the transmitter 40 is actuated. The initial synchronization value stored in every transmitter is zero, although it can be any number.

With reference to FIG. 3, a nonlinear function is used to generate the sixty-four bit "secret key" that is stored in a transmitter 40. The inputs to the nonlinear function are (a) the unique twenty-four bit serial number for the particular transmitter and (b) a sixty-four bit "manufacturers key". The same sixty-four bit "manufacturers key" is used to program each transmitter. The nonlinear function uses the "manufacturer's key" and the serial number to generate a unique sixty-four bit "secret key" which is stored in the transmitter. The unique serial number is also directly stored in the transmitter 40.

With reference to FIG. 4, there is now described the initial programming of the receiver 42. The receiver 42 is initially programmed with the sixty-four bit "manufacturers key". The receiver 42 is also programmed with (1) a temporary sixty-four bit "secret key", (2) a temporary synchronization value, (3)

a temporary button value and (4) a temporary check value at the factory for test purposes. However, this temporary sixty-four bit "secret key" and the other temporary values do not correspond to those of any particular transmitter 40.

The Encryption/Decryption Process

The encryption process is used to generate a thirty-two bit changeable hopping code which is transmitted by each transmitter to the receiver 42. The encryption process is carried out by the encoding circuitry 48 using a code hopping non-linear function.

Referring to FIG. 5, the inputs for the code hopping non-linear function are illustrated. The inputs include: (a) the sixty-four bit "secret key" for the particular transmitter, (b) the synchronization value, (c) the button value and (d) the "check" value. The sixty-four bit "secret key", the synchronization value and the check value are the same as those described above.

The so-called button value is used to distinguish between the various buttons 44 on the transmitter. The transmitter 40 in the present embodiment of the invention can have up to four separate buttons 44 that can be pressed by the user. The additional buttons can be used to control other devices, such as gates, lights and other door operators. The button value is not programmed by the manufacturer because it is built into the hardware.

The output from the non-linear function is a thirty-two bit hopping code. Since the synchronization value changes each time the button 44 of the transmitter is pressed, the thirty-two bit hopping code changes with each transmission by the transmitter 40.

The decryption process is performed by the decoding circuitry 56 located in the receiver 42. With reference now to FIG. 6, the decryption process is performed using a code hopping non-linear function. The inputs for the non-linear function are: (a) the sixty-four bit "secret key" which will correspond to the one in the transmitter and (b) the thirty-two bit hopping code received from the transmitter. The sixty-four bit "secret key" is generated and stored in the memory 58 used by the decoding circuitry 56 of the receiver 42 by means of an

algorithm during the learn mode as explained below. The outputs from the code hopping non-linear inverse function are (a) the synchronization value (b) the button value, and (c) the check value. These three values correspond to those associated with the transmitter 40 from which the thirty-two bit hopping code was received.

Data Formats

FIG. 7a is an illustration of the data format of the coded signal transmitted by a transmitter 40. The same data format is always transmitted, regardless of whether the system is in the learn mode or the operate mode. The changeable thirty-two bit hopping code changes with each transmission.

The twenty-four bit serial number is unique to each particular transmitter 40, is stored in the transmitter 40 during the initial programming and does not change from one transmission to the next. The preamble and start bit are the same for each transmission.

The data format of the codes used for processing in the receiver 42 varies depending upon whether the receiver 42 is in the learn mode or the operate mode. FIG. 7b is an illustration of the data format of the coded signal used for processing in the receiver 42 in its learn mode. The twenty-four bit serial number is the unique, nonchanging serial number that was stored in the particular transmitter 40 (*i.e.*, the one transmitting) during the initial programming. As was discussed above, the thirty-two bit hopping code is different for each transmission by the transmitter 40.

FIG. 7c is an illustration of the data format of the coded signal used for processing by the receiver during its operate mode. The thirty-two bit hopping code received by the receiver 42 during the operate mode changes with each transmission. The twenty-four bit serial number transmitted by the transmitter 40 is not used by the receiver 42 during the operate mode.

Conditioning the Receiver Between the Operate Mode and the Learn Mode

A learn mode button 60 and a flash indicator 60′ are located on the exterior of power head 20, as shown in FIG. 1. The learn mode button 60 is connected to circuitry 56 in the receiver 42 and is used to place the microprocessor 55 in the learn mode. Before learn mode button 60 is pressed, the microprocessor remains in the operate mode. When the learn mode button 60 is pressed and released, the microprocessor 55 and related circuitry is placed in the learn mode for a predetermined period of time, for example thirty seconds, sufficient to allow the specific transmitter information to be received, calculated and processed.

When the learn mode button 60 is pressed and released, the flash indicator 60′ flashes, normally approximately two times per second, to show that the processor circuitry (and the system) is in the learn mode. The user of the system then presses the transmitter button 44 within the predetermined thirty second period, and the flash indicator 60′ remains illuminated (*i.e.*, does not flash) to show that the specific information from the transmitter is being received and processed.

The user must then press the transmitter button 44 again within a second predetermined period of time (*e.g*, thirty seconds) to confirm the information for the transmitter 40. The flash indicator 60′ will turn off when the information has been received and has been confirmed. The microprocessor 55 then automatically returns to the operate mode when the information has been confirmed, without the user pushing any button or taking any action.

Learn Mode

During the learn mode, the receiver 42 intercepts the thirty-two bit hopping code and the twenty-four bit serial number from the transmitter 40. The twenty-four bit serial number (received from the transmitter) and the sixty-four bit manufacturer's key (stored in the receiver at the factory) are then used to independently generate a sixty-four bit "secret key" that is identical to the sixty-four bit "secret key" of the particular transmitter.

The independently generated sixty-four bit "secret key" and the thirty-two bit hopping code received from the transmitter are then provided as inputs for the non-linear inverse code hopping function to decrypt the thirty-two bit hopping code and thus generate (1) a synchronization value, (2) a button value and (3) a check value. Finally, the independently generated sixty-four bit "secret key", the generated synchronization value, and the generated button and check values corresponding to information from the particular transmitter are stored in an unused location. The twenty-four bit serial number is not stored.

In accordance with a unique feature of the invention, the processing circuitry of the receiver automatically stores the sets of generated secret keys, synchronization, button and check values corresponding to the respective transmitters, randomly, and in unused locations within the memory 58. There is therefore no need to devise any type of means to "switch" between dedicated sections of memory in the receiver for respectively different transmitters.

More specifically, there are a total of seven "locations" in memory 58 for storing information corresponding to each transmitter in the receiver 42. Thus, such embodiment can be used with up to seven different transmitters per receiver. When the information corresponding to particular transmitter 40 is intercepted by the receiver 42, the receiver processing circuitry generates and stores its sixty-four bit "secret key" and the other information corresponding to that transmitter randomly in an unused memory location in the memory 58. If all seven memory locations are used, then information in one of the seven memory locations will be erased and replaced with the new information. Thus, the system of the present invention does not require an external, manually actuated switch for selecting the precise memory location in which the received "secret key" and the other information is to be stored.

Finally, the system of the present invention has an "erase-all" feature, which allows the user to erase all seven memory locations in the receiver memory 58. The "erase all" feature is activated by pressing the learn mode button 60 and holding it pressed for a minimum of eight seconds. After performing the erase-

all routine, all seven memory locations will be available, and it will be necessary to proceed through the learn mode steps again for each transmitter used with the system.

The Operate Mode

During the operate mode, the receiver 42 receives only the thirty-two bit hopping code transmitted by the transmitter 40. The system then sequentially decrypts the received hopping code using each sixty-four bit "secret key" that is stored in its memory 58.

More specifically, a first stored sixty-four bit "secret key" is used to decrypt the thirty-two bit hopping code, and the following checks are performed (in the order shown) to determine the validity of the decrypted code:

(1) The decrypted check value is compared to the stored check value to make sure they match exactly.

(2) The decrypted synchronization value is compared to the stored synchronization value. The decrypted synchronization value must fall within a "window" or range of acceptable values. The window is (ssv + 1) to (ssv + 15), where "ssv" is the stored synchronization value.

(3) The decrypted button value is compared to the stored button value to make sure they match exactly.

If any of the checks fail, a second stored sixty-four bit "secret key" is used to once again decrypt the thirty-two bit hopping code received from the transmitter 40. If this decryption also fails, a third stored sixty-four bit "secret key" is used to once again decrypt the thirty-two bit hopping code.

If all stored sixty-four bit "secret keys" fail, then the received thirty-two bit hopping code is determined not to be from an authorized transmitter, and the drive mechanism 64 will not be activated. However, if one of the stored sixty-four bit "secret keys" successfully decrypts the received thirty-two bit hopping code, the drive mechanism 64 is activated.

Finally, it is important to note that, since the window or range of acceptable values for the synchronization value is (ssv + 1) to (ssv + 15), the

system of the present invention will not operate if the transmitter 40 transmits the same code hopping signal on two successive occasions.

The Auto-Synchronization Routine

If the button switch 44 of a transmitter 40 is pressed more than a predetermined number of, say fifteen times when the transmitter 40 is out of the radio range of the receiver 42, the transmitter 40 and the receiver 42 will no longer be synchronized. The system of the present invention advantageously employs a procedure, called an auto-synchronization routine, for dealing with this problem.

When the receiver 42 receives a transmission from an "out-of-sync" transmitter 40, the sixty-four bit "secret key" will successfully decrypt the thirty-two bit hopping code, and the resulting decrypted check value will match the stored check value for the transmitter. However, the decrypted synchronization value will not fall within the window of acceptable values, and the system will therefore not actuate the garage door or other barrier operator.

The microprocessor 55 recognizes that the check values did match, however, and it temporarily stores the decrypted synchronization value. The microprocessor 55 then awaits a second transmission, which is highly likely since the door did not actuate on the first transmission.

Upon receiving a second transmission from the out-of-sync transmitter, the microprocessor 55 will compare the decrypted synchronization value with the one that was temporarily stored from the previous transmission. If it is within a second, smaller window of acceptable values, then the system will operate the door, and the synchronization value stored in the receiver 42 for that transmitter will be reset to restore synchronization between the receiver 42 and the transmitter 40. The smaller window of acceptable values is (tssv + 1) to (tssv + 3), where "tssv" is the temporarily stored synchronization value from the previous transmission.

While the present invention has been described in connection with the preferred embodiment, it is not intended to limit the invention to the particular

form set forth, but on the contrary, it is intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.